**Policy 1.A. Membership of the Statewide Longitudinal Data System Committee**

The Statewide Longitudinal Data System (SLDS) Committee will be comprised of the following individuals:

- The chancellor of the board of higher education or the chancellor's designee;
- The superintendent of public instruction or superintendent of public instruction's designee;
- The chief information officer or chief information officer's designee;
- The director of the department of career and technical education or the director's designee;
- The director of job service North Dakota or the director's designee;
- The commissioner of commerce or the commissioner's designee;
- The director of the department of human services or the director's designee;
- The director of the North Dakota educational technology council;
- The director of the North Dakota council of educational leaders or the director's designee;
- The director of the North Dakota workforce development council or the director's designee; and
- Two members of the legislative assembly appointed by the chairperson of the legislative management.

The governor will appoint the chairperson of the committee. The committee may appoint advisory subcommittees.

Source: N.D.C.C. 15.1-02-18

**Policy 1.B. Mission of the Statewide Longitudinal Data System Committee**

The SLDS Committee will propose, develop and govern a system for sharing longitudinal data that will maximize the usefulness of management information to stakeholders and partners of North Dakota education, training, employment and service systems while protecting the privacy and security of personal information. To carry out its mission, the committee will be guided by the state's commitment to the following:

- Compliance with federal and state laws and regulations;
- Individual privacy;
- Data security; and
- Data accuracy and reliability.

**Policy 1.C. Authority and Responsibilities of the Statewide Longitudinal Data System Committee**

The SLDS Committee will establish and enforce policies governing access to and collection, storage, exchange, disclosure and use of data by and through the SLDS. The policies will be based on federal and state laws and regulations, as well as data governance best practices.

The SLDS Committee will provide reports as necessary to legislative committees. Reports to the Information Technology Committee, the Interim Committee on Education Issues, and Interim Committee on Economic Development are required and will include recommendations for further development of the SLDS, cost proposals, proposed legislation and data sharing governance.

The SLDS Committee, after consultation with the Information Technology Department, will:

a. report the terms and conditions under which a person may be granted authorized access to data through the SLDS to the Information Technology Committee;

b. mandate SLDS data protection practices, including requirements for encryption and staff training, that are designed to ensure the security of electronic and physical data;

c. provide for privacy and security audits of the statewide longitudinal data system;

d. establish protocols, including procedures for the notification of students and parents, in the event of a data breach involving the statewide longitudinal data system; and

e. mandate SLDS compliance with applicable data retention and disposition requirements; and

f. make annual training on data protection available to school district employees, employees of the North Dakota university system and its institutions, elected and appointed state and local education officials, and individuals who have access to the state longitudinal data system.

The SLDS Committee will review, approve and oversee the SLDS budget. The SLDS Committee may solicit and receive private and public funds to be appropriated on a continuing basis for support of the SLDS.

The SLDS Committee will designate an SLDS Program Manager who will report to the committee on SLDS matters.

The SLDS Committee may enter into contracts to carry out its responsibilities and carry out the functions of the SLDS. The SLDS Committee may delegate its authority to enter into contracts.

The SLDS Committee may make recommendations regarding data protection and privacy but does not set policy for state or local agencies, including Local or Regional Education Agencies.

Source: N.D.C.C. 15.1-02-18 and [new legislation]

**Policy 1.D. Statewide Longitudinal Data System Committee Voting**

A quorum of the SLDS Committee is one-half or more of the members of the committee, or any smaller number if sufficient for the committee to transact business. A quorum is required before a vote may be taken on any proposal. Each member of the SLDS Committee in attendance will have one vote. A proposal will pass if a majority of SLDS Committee members in attendance votes in favor of it.

**Policy 2. SLDS Administration and Staff Roles**

SLDS Program Manager

The SLDS Program Manager will be responsible for executive management of the SLDS. The Program Manager will report to the SLDS Committee, which will review the Program Manager's performance on an annual basis. The Program Manager's duties will include:

- Leading and overseeing the SLDS staff;
- Recommending and implementing long- and short-term plans for the SLDS;
- Recommending and implementing SLDS policies;
- Recommending an annual SLDS budget and ensuring operational expenses stay within budgets approved by the SLDS Committee;
- Serving as a liaison between SLDS staff and the SLDS Committee and between the SLDS Committee and third-parties;
- Communicating with Information Technology Department leadership to coordinate activities and infrastructure as appropriate;
- Ensuring the SLDS is appropriately organized and staffed to carry out its responsibilities effectively, timely and in compliance with applicable laws, regulations and policies;
- Demonstrating the highest standards of ethics and compliance and maintaining a commitment to compliance throughout the SLDS;
- Reporting all data breaches and significant compliance failures to the SLDS Committee along with recommendations for corrective actions;
- Ensuring data protection risk assessments are conducted and ensuring appropriate internal controls and data protection systems are in place and effectively aligned against identified risks; and
- Communicating material developments and concerns to the SLDS Committee.

As business needs or projects arise, the following roles may be filled:

Team Lead Role

The Team Lead will report to the Program Manager and will be responsible for day-to-day administration of the SLDS and supervision of SLDS staff. The Team Lead's duties will include:

- Maintaining frequent communication with the Project Manager to ensure the Project Manager is apprised of material developments and concerns;
- Assisting the Program Manager with preparing annual budgets and monitoring costs;
- Developing a training schedule for SLDS staff members, ensuring SLDS staff attend their assigned training and communicating training needs to the Program Manager;
- Coordinating staff and resources to maximize the efficiency and effectiveness of the SLDS and to meet project expectations and deadlines;
- Serving as a liaison between SLDS staff and the Program Manager as needed;
- Enforcing SLDS policies and maintaining a culture committed to compliance at the SLDS; and
- Carrying out other duties as assigned by the Program Manager.

Project Manager Role

Project Managers will report to the Team Lead. Project Managers' duties will include:

- Complying with applicable laws, regulations and SLDS policies;
- Developing and adhering to schedules for assigned projects;

- Managing costs, resources and logistics for assigned projects;
- Communicating material needs, schedule or cost deviations, and concerns to the Team Lead;
- Ensuring the Team Lead is appropriately apprised of material developments, timelines and progress for assigned projects; and
- Attending training as required by the Team Lead.

Researcher Role

Researchers will report to the Team Lead. Researchers' duties will include:

- Complying with applicable laws, regulations and SLDS policies;
- Attending training as required by the Team Lead;
- Performing statistical analysis of data as requested by the Team Lead or as necessary and appropriate for assigned projects; and
- Communicating material issues, concerns and other information to Project Managers and the Team Lead, as appropriate.

Business Intelligence Team Member Role(s)

The Business Intelligence Team members will report to the Team Lead. Business Intelligence Team members' duties will include:

- Complying with applicable laws, regulations and SLDS policies;
- Attending training as specified by the Team Lead;
- Assuming day-to-day responsibility for data protection, security, maintenance and retention;
- Developing and loading databases as directed;
- Creating reports as directed;
- Identifying data integrity issues; and
- Carrying out other duties as assigned by the Team Lead or Project Managers.

**Policy 3. Eligibility and Responsibilities of Data Providers**

Subject to state and federal laws and regulations as well as SLDS policies, public and private entities may provide data to the SLDS. Access to a Data Provider's data by or through the SLDS may be continual or limited to specific requests.

Each Data Provider will execute the appropriate data sharing agreement(s) governing the terms and conditions of access to and use of its data. The agreement(s) will incorporate appropriate breach notification requirements for SLDS and the Data Provider.

Each Data Provider will be responsible for the accuracy, quality, completeness and timeliness of the data provided.

Upon receipt of a request for data from SLDS or a Data Requester, a Data Provider will review the request and either approve it in writing or communicate any concerns regarding the request to SLDS and the Data Requester so the concerns can be addressed through good faith discussions among the relevant entities.

If the use of the Data Provider's data requires Institutional Review Board approval, the entity will cooperate with SLDS in seeking that approval.

A Data Provider will review any report(s) SLDS creates using the Data Provider's data in response to an approved data request. The Data Provider will review the report(s) in a timely manner before SLDS releases the report(s) to the Data Requester. The Data Provider will either approve the report(s) in writing or communicate any concerns regarding the report(s) to SLDS so the concerns can be addressed through good faith discussions among the relevant entities.

**Policy 4. Eligibility and Responsibilities of Data Requesters**

Subject to state and federal laws and regulations as well as SLDS policies, public and private entities may request data from the SLDS. Data may be accessed on continual basis or provided in response to a specific request.

Each Data Requester will submit to the SLDS a completed request form explaining the purpose(s) of the request, the specific data requested and the date by which the data are needed.

Each Data Requester will comply with the SLDS's and the Data Provider's requirements for data exchange and protection. These requirements will include but not be limited to:

- Execution of appropriate data sharing agreement(s) governing access to data provided by or through the SLDS;
- Secure transfer protocols;
- Data storage security protocols;
- Applicable limitations on access and re-disclosure;
- Cooperation with security and privacy audits;
- Cooperation with breach notification protocols; and
- Attendance at any training on data privacy and security mandated by the SLDS.

As necessary, Data Requesters will engage in good faith discussions with SLDS and Data Providers to address concerns about data requests and reports raised by Data Providers.

**Policy 5. Privacy and Security Audits**

SLDS personnel will conduct privacy and security audits of the SLDS and prepare a report of each audit for the SLDS Committee. The SLDS Program Manager will establish an audit protocol consistent with best practices. At a minimum, the following information and records will be included in reports of the audits:

- Review and validate that reports are available to list all users of the SLDS and its data by name and role of the individual;
- Verify security and authorization processes to grant access to the SLDS and its data are conducted annually by entities;
- Data fields collected, maintained or reported by the SLDS;
- Entities that provided data to the SLDS (Data Providers);
- Entities that requested data from the SDLS (Data Requesters);
- Data-sharing agreements that SLDS has executed;
- Date and scope of any identified data breaches;
- Summaries of responses, including notifications, of any identified data breaches, including inappropriate access to or release of individually-identifiable data;
- Summaries of any deviations from data transfer or storage protocols, including corrective actions taken;
- Summaries of any deviations from record retention and disposition policies, including corrective actions taken; and
- Dates and descriptions of data protection training offered by SLDS.

**Policy 6. Data Maintenance and Retention**

The SLDS will work with Data Providers and Data Requestors to identify data maintenance and retention requirements for longitudinal data. These requirements may vary based on the source, use or type of data at issue. To the extent applicable, the SLDS will follow the identified requirements. All SLDS personnel will be trained on applicable data maintenance and retention practices and requirements after they are identified and documented. Compliance with those practices and requirements will be audited.

**Policy 7.A. Data Protection and Privacy Generally**

The SLDS Committee and staff are committed to the highest standards of data protection and privacy. The SLDS Committee will monitor and evaluate changes in state and federal laws and regulations governing data protection and privacy on at least an annual basis. Compliance with those laws, as well as SLDS data protection and privacy policies and protocols, is mandatory. Non-compliance may result in disciplinary action, including termination from employment with the SLDS.

The SLDS Program Manager will coordinate with the Information Technology Department and others, as necessary, to identify and implement data protection best practices as well as to ensure the SLDS is utilizing the appropriate hardware and software to secure its data.

The Program Manager will ensure risk assessments and data protection audits are conducted as required by the SLDS Committee. The Program Manager will develop and ensure implementation of corrective actions for any material weaknesses identified through the risk assessments and audits.

All SLDS staff will attend data protection and privacy training upon their hire and at least annually thereafter. All staff will follow operational protocols and implement any corrective actions developed by the Program Manager or Team Lead. SLDS staff will be responsible for reporting material lapses in protocols and data breaches to the Team Lead or Program Manager.

Any other individual granted access to data maintained by or through the SLDS will attend data protection and privacy training and will certify they will comply with SLDS data protection and privacy policies and protocols. Non-compliance will result in termination of access.

**Policy 7.B. Data Protection and Privacy: Individually-Identifiable Data (also known as Personally-Identifiable Information)**

Data that identify or that reasonably can be used to identify an individual are protected by several federal and state laws and regulations. Additionally, North Dakota's open records laws prohibit the disclosure of information that is made confidential by law. The SLDS Committee and staff are committed to compliance with all data protection laws and regulations. Non-compliance may result in disciplinary action, including termination from employment with the SLDS and termination of access to SLDS data.

In cooperation with the Attorney General's Office, the Program Manager will oversee the development of protocols for accessing and releasing individually-identifiable data. SLDS staff will not access or release individually-identifiable data to anyone other than the Data Provider unless doing so is consistent with an approved protocol or else is approved by the Program Manager after consultation with legal counsel. To the extent necessary, the Program Manager will consult with legal counsel regarding access to or release of individually-identifiable data.

New hire and annual data protection and privacy training will describe protocols governing individually-identifiable data and explain relevant laws, including:

- Family Education Rights and Privacy Act (FERPA), which generally prohibits the disclosure of personally-identifiable information in education records;
- Health Insurance Portability and Accountability Act (HIPAA), which generally prohibits the disclosure of individually-identifiable health information;
- Federal and states laws governing unemployment compensation information; and
- State open records and confidentiality laws.